口座と取引のセキュリティ

口座のセキュリティは当社にとって重要であり、当社は、Remitlyの口座に関連する情報を守るため、対策を講じています。また、お客様ご自身でも、口座や個人情報の保護対策を実施いただけます。

口座確認プロセス

お客様のRemitly口座は、高レベルのセキュリティ、信用、保護を維持するため確認手順の対象となっております。

Remitlyの新規のお客様がRemitlyのウェブサイトを利用して新たなRemitlyの口座を開設される場合、お客様は特定の個人情報をご提供の上、電子メールで確認プロセスを完了いただく必要がございます。

お客様の口座の稼働開始後、当社は、手動および自動のさまざまなリスク管理手順を導入し、不審な口座の動きが明らかになるようにいたします。これは、お客様の過去のご利用と比較し、異常である、または矛盾すると思われる特徴を識別することを目的としています。このプロセスの一環として、個人情報や金融情報を確認するため、当社は業界をリードするサービスプロバイダーと契約を結んでいます。前述のサービスではお客様に直接ご連絡することはなく、お客様が希望される取引を正常に完了させること以外の目的で、お客様の情報を利用することはございません。

パスワードセキュリティ

お客様が口座にログインされる際、当社は、特定の措置を講じて口座を保護します。まず、お客様がRemitlyの口座にログインされる際には、必ず安全なサーバー接続（https://）によりログインが行われます。当社は、安全なサーバー保護で業界の標準である256ビット暗号化Secure Socket Layer（SSL）を使用しています。

また、お客様の口座は、ご自身で作成する固有のパスワードで保護されます。パスワードには一般的な単語や語句を使わないでください。代わりに、数字、大文字と小文字の両方使った8文字以上のパスワードを使うようにしてください。このパスワードは、外部に漏らさないようにしていただく必要がございます。パスワードを共有された場合、

お客様のRemitly口座のセキュリティが低下します。

インターネット詐欺にご注意ください

宝くじや懸賞の当選金を請求するため、または多額の金銭を受け取るという約束に対し、支払いを行わないでください。

クレジットカードやローンを「保証する」という謳い文句に対し、支払いを行わないでください。

本当かどうか疑問のあるインターネットや電話による申し出には、応じないでください。

知らない人、または身元が確認できない人に対し、支払いを行わないでください。

何らかの疑いを感じた場合は、要求された支払いの目的や安全性について、より詳しい情報を受取人に尋ねてください。取引に対し確信が持てるまでは、支払いを実行しないでください。

フィッシングメールまたはなりすましメールの識別

ときに、Remitlyから送られたように見えるが、実際にはそうではないメールが届くことがあります。このようなメールは、お客様をRemitlyのウェブサイトに似せたウェブサイトに誘導する場合があります。メールアドレスやパスワードといった口座情報を提供するよう、求められることすらあります。

こうした偽のウェブサイトでは、詐欺に利用するために、お客様の機密である口座情報や支払情報が盗まれる可能性があります。このような偽メールには、パスワードや機密データを検出することができるウイルスやマルウェアが含まれている可能性があります。そのため、当社では、ウイルス対策プログラムをインストールし、常に最新の状態に保つことをお勧めしています。

次の各項は、詐欺メール防御の一環として、留意すべき重要なポイントとなります。

以下の事項をRemitlyがメールでお尋ねすることはありません

社会保障番号（SSN）や生年月日

クレジットカード番号、PINコード、クレジットカードのセキュリティコード（上記のいずれかの「更新」を含む）

不審な電子メールの添付ファイルに警戒しましょう

当社では、不審な送信元または知らない送信元からの電子メールに添付されているファイルは開かないことをお勧めしています。電子メールの添付ファイルにはウイルスが含まれている場合があり、添付ファイルを開くとお使いのコンピューターが感染する可能性があります。添付ファイルが含まれていて、Remitlyを偽装したと思える不審なメールを受け取った場合、当社では、添付ファイルを開かずにそのメールを削除することをお勧めしています。

文法の誤りや誤字脱字を探しましょう

稚拙な文法上の誤りや、誤字脱字の有無を確認するようにしてください。フィッシングメールの中には、他の言語を翻訳し校正を行わずに送信されたものがあり、そのようなものには、文法上の誤りや誤字脱字が含まれています。

返信先のアドレスをチェックしましょう

[この電子メールは、本当にRemitlyからであるかを確認してください。フィッシング詐欺では、Remitlyから送られたかのように偽装した電子メールが送信されますが、返信アドレスを確認することで、本物かどうか判断できる場合があります。メールの「from」の行に「remitly-security@hotmsil.com」あるいは

「remitlyfraud@msn.com」のように書かれていたり、他のインターネットサービスプロバイダーの名称が含まれていたりする場合、それは本物ではありません。]
(mailto:remitly-security@hotmail.com)

ウェブサイトアドレスを確認しましょう

[**本物のRemitlyのウェブサイトは、必ず「http://www.remitly.com/」のドメインの中に存在します。**](https://www.remitly.com/)

なりすましメールに含まれているリンクがRemitlyの本物のアドレスに見えることがあります。リンクの上にマウスオーバーするとリンクが実際に指している場所をチェックできます - 実際に指している場所のウェブサイトは、ブラウザ画面の下部のステータスバーやポップアップに表示されます。

[**当社は上記以外のドメインでの中にあるウェブアドレスは決して使いません。たとえば、「http://security-payments-remitly.com/...」のような変形ドメインや「http://123.456.789.123/remitly.com/...」といったIPアドレス（数字の文字列）の後にディレクトリが続くものは、有効なRemitlyのアドレスではありません。**](https://security-payments-remitly.com/)

また、時には、テキストのどこかをクリックすると、詐欺サイトに誘導するように設定されたなりすましメールも存在します。Remitlyがこのようなメールを送信することは決してありません。このようなメールで偶然クリックしてしまい、偽サイトに誘導された場合は、何も情報を入力せず、ブラウザ画面を閉じてください。

電子メールが疑わしい場合は、直接Remitlyのウェブサイトにアクセスしてください。

[**疑わしいと感じたら、メールの中のリンクをクリックしないでください。http://www.remitly.com/に直接アクセスして右上のメニューからお客様の口座をクリックし、最近の購入を表示するか、口座情報を確認するようにします。口座にアクセスできない場合や、何か疑わしいことがある場合は、すぐに当社に知らせてください。**]
(https://www.remitly.com/)

口座情報の保護

[**なりすましメールや疑わしいメールをクリックし、その結果Remitlyの口座情報を入力してしまった場合は、ただちにパスワードを更新する必要があります。更新を行うには、http://remitly.comに直接アクセスし、口座設定をクリックしてください。次のページで、個人情報、電子メールアドレスまたはパスワードの変更をクリックします。**](https://www.remitly.com/)

偽装メールにリンクしているサイトからクレジットカード番号を送信してしまった場合、当社では、ご自身の情報を保護する措置を講じるよう、アドバイスしています。たとえば、クレジットカード会社に連絡を取って、この件について伝えます。最終的には、ご自身のRemitlyの口座からそのクレジットカードを削除し、誰もお客様の口座に不正にアクセスできないようにする必要があります。

フィッシングメールの報告

[**メールを受信してなりすましメールだと気づいた場合、あるいはフィッシング攻撃の被害を受け、ご自分のRemitly口座が心配だと思われた場合、すぐにフィッシングメールやなりすましメールについて当社にご報告ください。**](https://www.remitly.com/jp/ja/home/contact/)